UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN
SOUTHERN DIVISION

UNITED STATES OF AMERICA,

Plaintiff,

Criminal Action No. 16-20006
Honorable Victoria A. Roberts
Magistrate Judge David R. Grand

v.

PATRICK PINCHOT,

Defendant.
_____/

**REPORT AND RECOMMENDATION TO DENY DEFENDANT'S MOTION TO SUPPRESS EVIDENCE [19]**

On January 6, 2016, Patrick Pinchot ("Pinchot") was charged in an indictment with one count of Coercion and Enticement of a Minor, 18 U.S.C. § 2422(b); one count of Production of Child Pornography, 18 U.S.C. § 2251(a); one count of Receipt of Child Pornography, 18 U.S.C. § 2252A(a)(2); one count of Transfer of Obscene Material to a Minor, 18 U.S.C. § 1470; and one count of Possession of Child Pornography, 18 U.S.C. § 2522A(a)(5)(B). On February 23, 2016, Pinchot filed a motion to suppress evidence [19], which has been referred to this Court for a Report and Recommendation pursuant to 28 U.S.C. § 636(b)(1)(B). [20]. The government filed a response [21], and Pinchot filed a reply [22]. Because the Court finds that the issues are adequately presented in the parties' briefs, it dispenses with oral argument pursuant to E.D. Mich. L.R. 7.1(f)(2).[1] For the following reasons, the Court RECOMMENDS that Pinchot's

[1] The Court declines to conduct an evidentiary hearing with respect to the instant motion as there are no "contested issues of fact going to the validity of the search [that] are in question." *United States v. Abboud*, 438 F.3d 554, 577 (6th Cir. 2006) (citation and internal quotation marks omitted). Since Pinchot challenges the sufficiency of the allegations supporting the magistrate judge's probable cause determination, the instant motion strictly poses a legal question that can

motion [19] be DENIED.

**BACKGROUND**

On December 4, 2015, Federal Bureau of Investigation Special Agent Brian Conolly ("Conolly") swore to an affidavit before a United States Magistrate Judge, the purpose of which was to seek permission to search two residences associated with Pinchot, 939 Moran Ave., in Lincoln Park, Michigan, and 15809 Jonas Ave., in Allen Park, Michigan. Conolly averred, and the magistrate judge agreed, that the affidavit established probable cause that Pinchot had violated 18 U.S.C. §2252A(a)(2) (receipt of child pornography), and 18 U.S.C. §2252A(a)(5)(b) (possession and access with intent to view child pornography), and that evidence of those crimes would be found at those two addresses.

Agent Conolly explained that in late February 2015, a U.S. Probation Officer was conducting a home visit of "Individual 1" (a person other than Pinchot), a sex offender on supervised release from a 2009 child pornography conviction. The Probation Officer located an unauthorized cell phone in Individual 1's possession. A forensic analysis of the phone was conducted, which "revealed KIK messages evidencing Individual 1's receipt and distribution of child pornography to approximately 157 additional KIK users, including username "**looking4younggirls**."[2] Further forensic analysis revealed that "looking4younggirls" participated in a KIK chat session with over 100 KIK users, many of which had usernames that

---

be appropriately resolved by evaluating "the information presented in the four corners of the affidavit." *United States v. Jackson*, 470 F.3d 299, 306 (6th Cir. 2006); *see also United States v. Knowledge*, 418 F. App'x 405, 408 (6th Cir. 2011) (stating that "[a] defendant is not entitled to an evidentiary hearing where his arguments are entirely legal in nature.").

[2] Agent Conolly provided the following details about the Kik Messenger program: "KIK Messenger is a free, instant messaging application for mobile devices…KIK uses usernames, not phone numbers, as the basis for KIK accounts, chats, and other communications…KIK is primarily used as a cell phone application."

indicated an interest in child pornography such as the account in question here ("looking4younggirls"), "youngpedolover," "fuckthemyoung," "babyfucker," and "tradelilgirlnudes." This KIK chat session occurred between February 17-24, 2015, and involved the sharing of child pornographic images/videos, and discussion indicating an interest in that material. According to Agent Conolly's affidavit, forensic analysis revealed the following "subsets" of this chat session: "On February 17, 2015, 'adaddyslove' posted four (4) [child pornographic images]. 'fire301' then asked 'Who is she,' to which 'adaddyslove' responded 'My little friend.' 'fire301' then asked 'How old, if I may ask,' to which 'adaddyslove' responded '12'. '**Looking4younggirls**' then asked 'Video?' 'SGSIL' then shared a file depicting a real minor female child performing oral sex on an adult male. '**looking4younggirls**' then wrote: 'Of the 12yo I mean. Lol.[3]'"

Administrative subpoenas were served on KIK Interactive Inc, seeking account information for "lookingforyounggirls." KIK advised that the user of "lookingforyounggirls" was associated with the user of "Suppix.Records@gmail.com," and provided three login IP addresses associated with the account. In turn, administrative subpoenas were issued to the internet service providers for these IP addresses; two resolved back to residences associated with Pinchot (the two addresses which were the subject of Agent Conolly's subpoena) and the third to

[3] Although this appears to be the last comment posted by "looking4younggirls" in the group chat session in question, Agent Conolly states that the chat session continued for about another week, with various members describing, in graphic detail, the type of child pornography they would like to see, and sharing dozens of images of child pornography. While "looking4younggirls" may have had access to and actually received and seen those subsequent communications and images, this Court's analysis would be no different even if that were not the case. Accordingly, it will only consider the *contents of the chat session* through "looking4younggirls'" last post ("Of the 12yo I mean. Lol."). The Court notes, however, that "looking4younggirls" "utilized [KIK] every day during the time period November 9, 2015 through November 22, 2015." And, at some point between February 2015 and November 9, 2015, "looking4younggirls" changed the first and last name associated with the account from "MarriedM4" (first name) "young girls only" (last name) to "DaddyLikesGirls" (first name) "11 and up" (last name).

his employer's business address.

Agent Conolly averred that after Pinchot was identified as being associated with the addresses in question, it was determined that he had been the subject of police reports in 2006 and 2007, and in each case he was charged with criminal sexual conduct related to the sexual molestation of young girls.[4]

In his affidavit, Agent Conolly next discusses "Characteristics of Pornography Participants," and states, "…I have discussed the aspects of computers and their relationship with child pornography offenses with others…there are certain characteristics common to individuals involved in the receipt and collection of child pornography." Agent Conolly then wrote:

> 23. * * *
>
> a. Individuals who receive and collect child pornography may receive sexual gratification … viewing children engaged in sexual activity…Based on the evidence obtained in this investigation, images viewed and accessed via KIK messenger by a cell phone that has utilized IP address at [Pinchot's addresses] depicted [child pornography];
>
> b. Individuals who receive and collect child pornography do so in a variety of media, including, but not limited to, digital images and videos of child pornography. Based on the evidence obtained in this investigation, a cell phone that accessed the internet from [Pinchot's addresses] had access to numerous files that were indicative of containing child pornography;
>
> c. Individuals who receive and collect child pornography almost always possess and maintain their 'hard copies' of child pornography … in [] their home or other secure location. Maintaining these collections in a digital or electronic format in a safe, secure and private environment, such as a computer in a private residence, allows the collectors the opportunity to safely maintain their collections for many years and enable the collector to frequently view the collection…In this case, it is highly likely that [] Pinchot's cell phone contains child pornography…As a child pornography collector, Pinchot may also store child pornography on

[4] Agent Conolly's affidavit does not indicate the disposition of these charges.

other electronic media, including personal computers and tablets;

d. Child pornography collectors may also correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors…and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography. Based on the evidence obtained in this investigation, an individual used the IP address associated with [Pinchot's addresses] to access KIK messenger, an application that he also used to view and access child pornography.

24. Based on my training and experience and my conversations with other investigations, child pornography collectors typically retain pictures, films, photographs …at their private residence, for many years. The nature of the materials…motivates collectors to keep their child pornography collection within their possession and control wherever they go.

In the next section of his affidavit, entitled "Background on Computers and Child Pornography," Agent Conolly described the capabilities of computers in terms of storing electronic media and images. He noted that, "As is the case with most digital technology, communications by way of a computer can be saved or stored on the computer used for these purposes…Storing this information can be intentional…[or accomplished] unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places (e.g., temporary files or ISP software)…"

In a section of his affidavit entitled, "Specifics of Search and Seizure of Computer Systems," Agent Conolly explained that "[s]earches and seizures of evidence from computers commonly require agents to download or copy information from the computers [], or seize most all computer items … [because] Computer storage devices [] can store the equivalent of thousands of pages of information…[and] Searching computer systems for criminal evidence is a highly technical process requiring expert skill …" Agent Conolly further stated, "there is probable cause to believe that the computer and its storage devices are all instrumentalities of the

[child pornography crimes] crime(s) … and should all be seized."

Agent Conolly concluded his affidavit by stating that, "there is probable cause to believe that [] Pinchot, who resides at [the two residences referenced above] has violated 18 U.S.C. § 2252A(a)(2) (receipt of child pornography), and 18 U.S.C. § 2252(a)(5)(B) (possession and access with intent to view child pornography)." He averred that there is probable cause that evidence of those crimes would be found at the two residences associated with Pinchot, and that the evidence sought is "contraband, the fruits of crime…or property which is or has been used as the means of committing the foregoing offenses." Exhibit B to Agent Conolly's affidavit was entitled, "List of Items to be Seized and Searched," which included the following:

> 1. All visual depictions, including still images, videos…of child pornography…and any mechanism used for the receipt or storage of the same, including, but not limited to:
>
> a. Any computer, computer system and related peripherals including and [sic] data processing devices and software (including but not limited to central processing units; internal and peripheral storage devices such as fixed disks…PDA's, gaming consoles, cell phones…"

After the search warrants in question were approved by a magistrate judge and signed, they were executed by agents. At one of the residences, they seized a computer, thumb drives, and two cell phones, both of which allegedly contained child pornography. Pinchot was interviewed and allegedly made a number of incriminating statements.

**PINCHOT'S MOTION TO SUPPRESS**

On February 23, 2016, Pinchot filed the instant motion to suppress. [19]. In support of his motion, Pinchot argues that Agent Conolly's affidavit failed to establish the requisite "nexus" between the places to be searched – *i.e.*, Pinchot's two residences – and the evidence sought "because the evidence relied upon in obtaining the search warrant was stale." [*Id.* at 4, ¶7; *id.* at

10 ("Mr. Pinchot contends that no such nexus can be established on the facts of this case because the evidence relied upon in seeking this warrant was almost 10 months old. In other words, the evidence was stale."]. Pinchot argues that the evidence was stale under the circumstances here, where he is accused of using a *cell phone* to access child pornography via the KIK Messenger program, and Agent Conolly's affidavit purportedly did not describe that program's transmission and storage capabilities sufficiently to allow the reader to find that the evidence being sought was likely to be found on Pinchot's cell phone:

> The allegations contained in SA Conolly's affidavit involved child pornography. Typically, because child pornography offenses are "carried out . . . over a long period, the same time limitations that have been applied to more fleeting crimes do not control the staleness inquiry . . . ." This is because collectors of child pornography typically retain and foster their collections for long periods of time on their computers.
>
> The rationale, however, crumbles under these facts because, unlike the majority of cases addressing this issue, the affidavit here does not allege Mr. Pinchot used a computer to access, distribute, or store child pornography. Instead, he is accused of using a cell phone to participate in a chat session through an application called KIK. Without information addressing whether KIK is capable of: 1) storing images for long durations; 2) transferring images to computers; 3) saving images on the phone[5]; 4) retrieving deleted images; or 5) whether the application can be accessed on a home computer; there is no basis to believe that ten month old text messages are "fresh" enough to find probable cause. Especially because the affidavit fails to allege any other criminal activity closer in time to the date the warrant was issued that would freshen the 10 month old information.

[19 at 11-13 (internal citations omitted)]. Similarly, in his reply brief, Pinchot argues that Agent Conolly's affidavit is insufficient because it "fails to describe anything about the unique nature of the KIK application and its storage capabilities. Instead, the warrant application addresses in

[5] Indeed, even the Supreme Court has recognized that "the data a user views on many modern cell phones may not in fact be stored on the device itself." *Riley v. California*, 134 S. Ct. 2473, 2491 (2014). (Footnote from Pinchot's brief as indicated in above block quote).

broad terms the unique capabilities of 'computers' in general, without any specific reference to cellphones or cellphone-based applications." [22 at 4].

The government, on the other hand, argues that "the nine-month time period between [Pinchot's] receipt of child pornography and the execution of the search warrants did not cause the probable cause to expire, given the inherent nature of child pornography crimes." [21 at 1]. Specifically, the government points to the fact that "many smart phones [have the ability] to store large amounts of information….It is very easy to transfer image and video files between smart phones and other devices." [*Id.* at 16]. They also point to certain facts contained in Agent Conolly's affidavit about Pinchot's alleged use of his cell phone, such as his continued use of the KIK username "looking4younggirls" through at least November 23, 2015, which was just a few weeks before the search warrant was approved and executed. [*Id.* at 17].

For the reasons discussed below, the Court finds that Pinchot's arguments lack merit, and his motion to suppress should be denied.

**APPLICABLE LEGAL STANDARDS**

Generally, before authorities may search a person's home or property, they must obtain a warrant. *United States v. Smith*, 510 F.3d 641, 647 (6th Cir. 2007). In turn, the Fourth Amendment provides that "no Warrant shall issue, but upon probable cause, supported by Oath or affirmation." U.S. Const. amend. IV. When considering an application and affidavit for a search warrant, "the task of the issuing magistrate judge is simply to make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before him, including the 'veracity' and 'basis of knowledge' of persons supplying hearsay information, there is a fair probability that contraband or evidence of a crime will be found in a particular place." *Illinois v. Gates*, 462 U.S. 213, 238 (1983). Thus, "[a] warrant will be upheld if the

affidavit provides a 'substantial basis' for the issuing magistrate to believe 'there is a fair probability that contraband or evidence of a crime will be found in a particular place.'" *Smith*, 510 F.3d at 652 (quoting *Gates*, 462 U.S. at 238).

As the Supreme Court explained in *Gates*, 462 U.S. at 232, probable cause is a "fluid concept—turning on the assessment of probabilities in particular factual contexts—not readily, or even usefully, reduced to a neat set of legal rules." Thus, "[c]ourts should review the sufficiency of the affidavit in a commonsense, rather than hypertechnical manner." *United States v. Greene*, 250 F.3d 471, 479 (6th Cir. 2001). "[R]eview of an affidavit and search warrant should rely on a 'totality of the circumstances' determination, rather than a line-by-line scrutiny." *Id.* (quoting *United States v. Allen*, 211 F.3d 970, 973 (6th Cir. 2000) (en banc)).

Further, "[t]o justify a search, the circumstances must indicate why evidence of illegal activity will be found 'in a particular place.' There must, in other words, be a 'nexus between the place to be searched and the evidence sought.'" *United States v. Carpenter*, 360 F.3d 591, 594 (6th Cir. 2004) (quoting *United States v. Van Shutters*, 163 F.3d 331, 336–37 (6th Cir. 1998)). "In addition, probable cause must exist at the moment that the warrant is issued and the evidence supporting it cannot be stale." *U.S. v. Whetstone*, 2009 WL 4506430, at *3 (E.D. Mich. Nov. 25, 2009) (citing *Sgro v. United States*, 287 U.S. 206, 210 (1932)). "There is no fixed time limit regarding the staleness of evidence and a court must consider the following variables: 'the character of the crime (chance encounter in the night or regenerating conspiracy?), the criminal (nomadic or entrenched?), the thing to be seized (perishable and easily transferable or of enduring utility to its holder?), the place to be searched (mere criminal forum of convenience or secure operational base?), etc.'" *Id.* (quoting *United States v. Spikes*, 158 F.3d 913, 923 (6th Cir.

1998)). "[R]eviewing courts are to accord the magistrate's determination 'great deference.'" *Allen*, 211 F.3d at 973 (quoting *Gates*, 462 U.S. at 236).

**ANALYSIS**

**A. Agent Conolly's Affidavit Established Probable Cause for the Searches**

First, Agent Conolly's affidavit established probable cause that Pinchot had committed the crimes of receiving child pornography and possession/access with intent to view child pornography, in violation of 18 U.S.C. §§ 2252A(a)(2) and 2252A(a)(5)(b), respectively. Evidence provided by various internet service providers showed that Pinchot was linked to the KIK user name "looking4younggirls," and evidence found on Individual 1's cell phone showed that "looking4younggirls" had participated in a KIK chat session with over 100 other KIK users, many of which, like Pinchot, had usernames that indicated an interest in child pornography. During the chat session, numerous videos/images of child pornography were shared amongst and viewed by the participants, including Pinchot. For instance, in one chat session "subset," "adaddyslove" posted four child pornography images, and a number of other participants then either made comments (one of which stated that the child in the photos was 12 years old) or, in Pinchot's case, asked questions ("Video?") about the images. Another user then posted a child pornographic video, and evidence suggests that Pinchot watched it because he "later wrote: 'Of the 12yo I mean. Lol.'"

But Pinchot does not seek to suppress the evidence found on Individual 1's cell phone. Rather, he seeks to suppress the evidence found at his home (and incriminating statements he made to officers there) when the warrants in question were executed. Again, his argument is that "the evidence relied upon in obtaining the search warrant was stale" because the above-referenced chat session occurred about 10 months before the warrant was approved/executed,

and because "he is accused of using a cell phone to participate in a chat session through [] KIK," when Agent Conolly's affidavit failed to address "whether KIK is capable of: 1) storing images for long durations; 2) transferring images to computers; 3) saving images on the phone…" [19 at 4, ¶7; *id.* at 10-13 (internal citations and footnote omitted)]; *see also* 22 at 3 ("there is no information that the KIK application is capable of storing or retrieving images")]. This argument misses the mark as its premise is incorrect.

Agent Conolly's affidavit did provide factual information demonstrating that the KIK program was capable of storing/retrieving images on cell phones; he averred that agents conducting a "forensic analysis of [Individual 1's] cellular phone" in late February 2015 found the February 17-24, 2015 KIK chat session, and were able to retrieve the child pornographic images and videos from that chat session, including the ones Pinchot had seen. Given that this electronic evidence remained on Individual 1's cell phone for at least a week, and given the nature and capabilities of today's cell phones, it was reasonable for the magistrate judge to conclude that evidence of Pinchot's participation in the chat session would remain on (or at least could be retrieved from) his cell phone, even 10 months after the fact.

This conclusion is supported by the U.S. Supreme Court's discussion of modern cell phones' capabilities in the recent case of *Riley*, 134 S.Ct. at 2489; "The term 'cell phone' is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone…One of the most notable distinguishing features of modern cell phones is their immense storage capacity."[6] Other aspects of Agent Conolly's

[6] As noted above, Pinchot cites *Riley* for its statement that "the Supreme Court has recognized that 'the data a user views on many modern cell phones may not in fact be stored on the device itself.'" *Riley*, 134 S. Ct. at 2491. [19 at 12 n.6]. As this Court just explained, however, Individual 1's cell phone was able to store the KIK chat session and child pornographic images and videos, and it was therefore reasonable for the magistrate judge to conclude that whatever

affidavit speak to this point. In providing "Background on Computers and Child Pornography," Agent Conolly noted that, "As is the case with most digital technology, communications by way of a computer can be saved or stored on the computer…" Since a cell phone is clearly a form of "digital technology," one can reasonably understand Agent Conolly to be saying that electronic communications transmitted over a cell phone can be saved to the cell phone, and thus are retrievable from the cell phone. In fact, Agent Conolly clearly considered a cell phone to be a type of computer; in describing "Characteristics of Pornography Participants," he averred, "Maintaining [child pornography] collections in a digital or electronic format in a safe, secure and private environment, ***such as a computer*** in a private residence, allows the collectors the opportunity to safely maintain their collections for many years…In this case, it is likely that [] ***Pinchot's cell phone*** contains child pornography." (Emphasis added). And, Agent Conolly provided factual information about "[i]ndividuals who receive and collect child pornography," averring that they "almost always possess and maintain their 'hard copies' of child pornography … in [] their home or other secure location."

While the foregoing alone establishes the warrant's validity, the government also cites to numerous Sixth Circuit cases for the proposition that because child pornographic images "typically persist in some form on a computer hard drive even after [manual deletion] and ... can often be recovered by forensic examiners," *United States v. Terry*, 522 F.3d 645, 650 n. 2 (6th

---

device Pinchot was using to participate in that chat session would have those same capabilities. Moreover, the Supreme Court's concern in *Riley* was not the risk that a search of one's cell phone might reveal too little (or nothing at all), but that it might reveal far more than could be tolerated in the absence of a warrant. *Riley*, 134 S.Ct. at 2490-91 ("In 1926, Learned Hand observed [] that it is 'a totally different thing to search a man's pockets and use against him what they contain, from ransacking his house for everything which may incriminate him.' If his pockets contain a cell phone, however, that is no longer true. Indeed, a cell phone search would typically expose to the government far *more* than the most exhaustive search of a house…") (emphasis in original) (internal citation omitted).

Cir. 2008), time periods similar to that in issue here (about 10 months) have not created "staleness" problems where a computer was used to access child pornography. [21 at 15-16 (citing *e.g.*, *United States v. Lewis*, 605 F.3d 395, 402 (6th Cir. 2010) (probable cause not stale where defendant sent images of child pornography to an undercover agent more than seven months before the search warrant application); *United States v. Frechette*, 583 F.3d 374 (6th Cir. 2009) (search warrant valid where defendant subscribed to child pornography website for one month, 16 months prior to the search); *United States v. Lapsins*, 570 F.3d 758, 767 (6th Cir. 2009) (finding probable cause despite nine-month lapse between police obtainment of illicit images linked to defendant and filing of warrant application); *United States v. Hampton*, 504 F. App'x 402 (6th Cir. 2012) (probable cause not stale where warrant was executed over 10 months after authorities observed child pornography shared through specific IP address)).

Pinchot argues that the cases on which the government relies are distinguishable from his case because they "all [] involve[d] defendants storing child pornographic images on their computers and engaging in conduct far more involved than Mr. Pinchot..." [22 at 4]. He notes, for instance, that two of the cases "involved defendants who used their computers to subscribe to child pornographic websites" and "download" child pornographic images. And, in two other cases, argues Pinchot, "the defendants actually sent or offered to send child pornographic images from their computer to interested parties." [*Id.*]. He notes that in each of these cases, the court relied largely on the proposition that such images remain on a *computer* for long periods of time, if not indefinitely. [*Id.* at 5-7]. Pinchot's attempt to distinguish these cases from his fails, though, because, as discussed above, Agent Conolly presented sufficient factual evidence from which the magistrate judge could reasonably conclude that, just like Individual 1, the cell phone Pinchot used to participate in the KIK chat was likely to contain evidence of child pornography,

even ten months after the fact. Moreover, although Pinchot's conduct could arguably be characterized as "less involved" than the defendants in the other cases, it was plenty "involved" to support the magistrate judge's approval of the warrant. Agent Conolly presented evidence demonstrating that Pinchot had a desire to obtain child pornography and that he acted on that desire by participating in the chat session centered around the exchange of child pornographic images, and by specifically requesting another user post a child pornographic video ("Videos?"). The fact that Pinchot's participation was via the KIK Messenger program rather than through a particular website is immaterial, particularly where evidence of the child pornography exchanged during the KIK chat was found on Individual 1's cell phone.

Thus, all of the staleness considerations outlined in *Spikes*, 158 F.3d at 923, weigh in favor of upholding the warrant and searches: the affidavit provided evidence of Pinchot's participation in an electronic crime involving his request for, receipt, and viewing of child pornography and averred that such participants "almost always possess and maintain their 'hard copies' of child pornographic material…in the privacy and security of their home." Under the "totality of the circumstances" described in Agent Conolly's affidavit – Pinchot's (and others participants') KIK user names openly projecting an interest in child pornography, his active participation in the KIK chat session involving the transmission of child pornographic images and videos, the fact that the chat session (including the images and videos) was later recovered from Individual 1's cell phone, the fact that persons who receive child pornography "almost always" keep it in their homes, and the capabilities of computers and other "digital technology" – the search warrant provided a "substantial basis" for the magistrate judge to believe there was a "fair probability" that the evidence being sought would be found in the locations to be searched. Accordingly, Pinchot's motion should be denied.

**B. The "Good Faith" Exception to the Exclusionary Rule Applies**

Even if Agent Conolly's affidavit failed to provide the requisite probable cause for the searches which were conducted, the evidence seized should not be suppressed because the agents who executed the searches acted in good faith. In general, the Fourth Amendment's "exclusionary rule" provides that evidence seized pursuant to an invalid search warrant must be suppressed. *See Weeks v. United States*, 232 U.S. 383 (1914); *Mapp v. Ohio*, 367 U.S. 643 (1961). However, because "the purpose of the exclusionary rule, which is to deter police misconduct, will not be served by excluding evidence seized by an officer acting in good faith," *United States v. Frazier*, 423 F.3d 526, 533 (6th Cir. 2005) (citing *United States v. Leon*, 468 U.S. 897, 916 (1984)), a "good-faith" exception to that rule exists. Thus, even if a search warrant is later held to be constitutionally deficient, evidence seized as a result of the search will not be suppressed if the officers executing the warrant had an "objectively reasonable" good-faith reliance on the magistrate judge's determination that probable cause existed. *Frazier*, 423 F.3d at 533; *Leon*, 468 U.S. at 905, 922. "In making this determination, all of the circumstances ... may be considered." *Leon*, 468 U.S. at 922–23 n. 23. The United States Supreme Court has highlighted four situations where this "good faith" exception is inapplicable:

> first, if the issuing magistrate "was misled by information in an affidavit that the affiant knew was false or would have known was false except for his reckless disregard for the truth;" second, if "the issuing magistrate wholly abandoned his judicial role;" third, if the affidavit was "so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable," or in other words, where "the warrant application was supported by [nothing] more than a 'bare bones' affidavit," and, fourth, if the "warrant may be so facially deficient—i.e., failing to particularize the place to be searched or the things to be seized."

*United States v. Weaver*, 99 F.3d 1372, 1380 (6th Cir. 1996) (citations omitted) (quoting *Leon*, 468 U.S. at 914-15, 923).

In arguing against applying the good faith exception to the searches in question, Pinchot contends:

> The third situation exists here because the warrant affidavit so lacked the requisite indicia of probable cause that it was "entirely unreasonable" for an official to rely on it. The warrant affidavit omitted essential basic facts about the KIK application that would have assisted this Court in determining the likelihood that Mr. Pinchot had child pornography in his home. Because the application was devoid of particularized facts needed for probable cause, the officers were unreasonable in relying on it, and the good faith exception does not apply.

[19 at 14].

Pinchot's conclusory assertions about a lack of "particularized facts" and "unreasonable" reliance by the officers lack merit. Again, Agent Conolly's affidavit specifically stated that Individual 1's cell phone contained evidence of the KIK chat session in question, and it was therefore reasonable for them to assume that Pinchot's cell phone would have the same capabilities and contain the same evidence. Additionally, the Court notes that Pinchot, through the "looking4younggirls" user name, "utilized [KIK] every day during the time period November 9, 2015 through November 22, 2015." And, at some point between February 2015 and November 9, 2015, "looking4younggirls" changed the first and last name associated with the account from "MarriedM4" (first name) "young girls only" (last name) to "DaddyLikesGirls" (first name) "11 and up" (last name). Coupled with all of the other evidence discussed herein, Pinchot's continued use of the KIK program via user names which openly projected an interest in child pornography suggests that he continued to search for child pornography via KIK in the days leading up to the search warrants' execution, and that such material was likely to be found where the agents were searching. Thus, the Court finds that the agents acted in good faith in relying on Agent Conolly's affidavit when they performed the searches in question.

**CONCLUSION**

For all of the foregoing reasons, the Court RECOMMENDS that Pinchot's motion to suppress evidence [19] be DENIED.

Dated: April 28, 2016
Ann Arbor, Michigan

s/David R. Grand
DAVID R. GRAND
United States Magistrate Judge

**NOTICE TO THE PARTIES REGARDING OBJECTIONS**

The parties to this action may object to and seek review of this Report and Recommendation, but are required to act within fourteen (14) days of service of a copy hereof as provided for in 28 U.S.C. § 636(b)(1) and Fed. R. Civ. P. 72(b)(2). Failure to file specific objections constitutes a waiver of any further right of appeal. *Thomas v. Arn*, 474 U.S. 140 (1985); *Howard v. Secretary of HHS*, 932 F.2d 505, 508 (6th Cir.1991); *United States v. Walters*, 638 F.2d 947, 949–50 (6th Cir.1981). The filing of objections which raise some issues, but fail to raise others with specificity, will not preserve all the objections a party might have to this Report and Recommendation. *Willis v. Secretary of HHS*, 931 F.2d 390, 401 (6th Cir.1991); *Smith v. Detroit Fed'n of Teachers Local 231*, 829 F.2d 1370, 1373 (6th Cir.1987). Pursuant to E.D. Mich. LR 72.1(d)(2), a copy of any objections is to be served upon this magistrate judge. A party may respond to another party's objections within 14 days after being served with a copy. *See* Fed. R. Civ. P. 72(b)(2); 28 U.S.C. §636(b)(1). Any such response should be concise, and should address specifically, and in the same order raised, each issue presented in the objections.

**CERTIFICATE OF SERVICE**

The undersigned certifies that the foregoing document was served upon counsel of record via email addresses the court has on file.

s/Eddrey O. Butts
EDDREY O. BUTTS
Case Manager

Dated: April 28, 2016